

EXHIBIT 1

State of Minnesota
Scott County

District Court
First Judicial District

Court File Number: **70-CV-21-11814**

Case Type: Civil Other/Misc.

FILE COPY

**Notice of Judicial
Assignment**

Elizabeth Lutz, individually and on behalf of all others similarly situated vs Electromed, Inc.

This case is assigned to:

Judge Martin Fallon
200 4th Avenue West JC 115
Shakopee MN 55379
952-496-8200

All future hearings shall be scheduled before this judicial officer.

Please note that a notice to remove this judicial officer must comply with Minnesota Rules of Civil Procedure 63.03 and Minnesota Statute § 542.16.

Dated: September 20, 2021

Vicky L. Carlson
Court Administrator
Scott County District Court

cc: Electromed, Inc.
BRYAN L BLEICHNER

State of Minnesota
Scott County

District Court
First Judicial District

Court File Number: 70-CV-21-11814

Case Type: Civil Other/Misc.

Notice of Remote Zoom Hearing

FILE COPY

Elizabeth Lutz, individually and on behalf of all others similarly situated vs Electromed, Inc.

You are notified this matter is set for a remote hearing. This hearing will not be in person at the courthouse.

<i>Hearing Information</i>
October 13, 2021
Case Management Conference
9:30 AM

The hearing will be held via Zoom and appearance shall be by video and audio unless otherwise directed with Judicial Officer Martin S. Fallon, Scott County District Court.

The Minnesota Judicial Branch uses strict security controls for all remote technology when conducting remote hearings.

You must:

- Notify the court if your address, email, or phone number changes.
- Be fully prepared for the remote hearing. If you have exhibits you want the court to see, you must give them to the court before the hearing. Visit www.mncourts.gov/Remote-Hearings for more information and options for joining remote hearings, including how to submit exhibits.
- Contact the court at 952-496-8200 if you do not have access to the internet, or are unable to connect by video and audio.

To join by internet:

1. Type <https://zoomgov.com/join> in your browser's address bar.
2. Enter the **Meeting ID and Meeting Passcode (if asked)**:
Meeting ID: 161 061 1721
Passcode: 947616
3. Update your name by clicking on your profile picture. If you are representing a party, add your role to your name, for example, John Smith, Attorney for Defendant.
4. Click the **Join Audio** icon in the lower left-hand corner of your screen.
5. Click **Share Video**.

To join by telephone (if you are unable to join by internet):

Be sure you know how to mute your phone when you are not speaking and unmute it again to speak.

1. Call Toll-Free: 1-833-568-8864
2. Enter the Meeting ID and Meeting Passcode:
Meeting ID: 161 061 1721
Passcode: 947616

Para obtener más información y conocer las opciones para participar en audiencias remotas, incluido cómo enviar pruebas, visite www.mncourts.gov/Remote-Hearings.

Booqo www.mncourts.gov/Remote-Hearings oo ka eego faahfaahin iyo siyaabaha aad uga qeybgeli karto dacwad-dhageysi ah fogaan-arag, iyo sida aad u soo gudbineyso wixii caddeymo ah.

Dated: September 20, 2021

Vicky L. Carlson
Scott County Court Administrator
200 4th Avenue West JC 115
Shakopee MN 55379
952-496-8200

cc: Electromed, Inc.
Bryan L Bleichner

State of Minnesota

County

Scott**District Court**

Judicial District:	First
Court File Number:	70-CV-21-11814
Case Type:	Civil Other/Misc.

**ELIZABETH LUTZ, individually and on
behalf of all others similarly situated,**

Plaintiff/Petitioner

vs/and

**Motion for Admission
Pro Hac Vice****ELECTROMED, INC.**

Defendant/Respondent

My name is Bryan L. Bleichner, and I am an active member in good standing of the bar of the State of Minnesota.

I move that this Court admit pro hac vice Terence R. Coates, who is an attorney admitted to practice in the trial courts of Ohio, but not admitted to the bar of this Court.

The proposed admittee will be counsel for the

☒ Plaintiff/Petitioner ☐ Defendant/Respondent in this case.

I am aware that Rule 5 of the Minnesota General Rules of Practice requires me to

1. Sign all pleadings in this case;
2. Accept service of all pleadings in this case; be present in person or by telephone at the proceeding at which this Motion is heard;
3. Be present before the court, in chambers or in the courtroom or if participating by permitted remote means in any hearing conducted by remote means; and
4. For a subsequent appearance in this case, pursuant to the court's discretion, the out-of-state attorney named above may conduct the proceedings without my presence.

09/27/2021

Dated

/s/ Bryan L. Bleichner

Signature

Name: Bryan L. Bleichner
 Atty Lic #: 0326689
 Law Firm: Chestnut Cambronne PA
 Address: 100 Washington Ave. So., Suite 1700
 Telephone: (612)339-7300
 Email: bbleichner@chestnutcambronne.com

State of Minnesota

County

Scott

District Court

Judicial District:

First

Court File Number:

70-CV-21-11814

Case Type:

Civil Other/Misc.

ELIZABETH LUTZ, individually and on
behalf of all others similarly situated,

Plaintiff/Petitioner

vs/and

Affidavit of Proposed AdmitteeELECTROMED, INC.

Defendant/Respondent

My name is Terence R. Coates, and I make the following statements in support of the motion for my admission pro hac vice.

1. ☒ I have not applied for *pro hac vice* admission in Minnesota in the preceding two years.

OR

- ☐ I have applied for *pro hac vice* admission in Minnesota in the **preceding two years**.

Please note: The Minnesota Board of Law Examiners only requires you to provide prior application information for the last 12 months, but Minn. Gen. R. Prac. 5.04(a) requires you to report prior application information for the preceding two years.

Details of each application are as follows:

Case Caption: _____

Venue: _____

Court File Number: _____

Was Admission Granted? _____

Case Caption: _____

Venue: _____

Court File Number: _____

Was Admission Granted? _____

If you have more than 2 prior applications, please use additional paper.

2. I am including a copy of the application to the Minnesota Board of Law Examiners submitted under Rule 5.03.
3. I am including a copy of the notice from the Minnesota Board of Law Examiners confirming good standing.

I declare under penalty of perjury that everything I have stated in this document is true and correct. Minn. Stat. § 358.116

9/25/2021
Dated

Hamilton County, Ohio
County and state where signed

Terence R. Coates
Signature

Name: Terence R. Coates
Atty Lic # 0085579 (Ohio)
and State:
Law Firm: Markowitz, Stock + DeMarco, LLC
Address: 3825 Edwards Rd., Suite 650, Cincinnati, OH 45209
Telephone: (513) 665-0204
Email: tcoates@msdlegal.com

ATTORNEY INFORMATION

Attorney Name	Terence	R.	Coates
	<i>First</i>	<i>Middle</i>	<i>Last</i>

FIRM INFORMATION

Firm Name	Markovits, Stock & DeMarco, LLC
Address	3825 Edwards Road, Suite 650 Cincinnati, Ohio 45209
Phone	(513) 665-0204
Email	tcoates@msdlegal.com

LICENSURE

Jurisdiction where you Primarily Practice	State of Ohio
Lawyer Registration Number in that Jurisdiction	0085579
Other Jurisdictions where license (if any) and Lawyer Registration Numbers in those Jurisdictions	United States District Court for the Southern District of Ohio (no registration number); United States District Court for the Northern District of Ohio (no registration number); United States District Court for the Eastern District of Michigan (no registration number).

Please enter NONE if not licensed in any additional jurisdictions.

Have you ever been licensed in Minnesota?	NO
Current state or foreign country of residence	State of Ohio
Certificate of Good Standing	<u>Coates Certificate of Good Standing (Aug. 19, 2021).pdf</u>

You must attach a certificate of good standing (PDF format only) from the attorney licensing authority in the Jurisdiction in which you primarily practice.

CASE RELATED

Name of Party you represent	Elizabeth Lutz
Case Number	70-CV-21-11814
Name of Minnesota Lawyer	Bryan L. Bleichner
<i>Name of Minnesota Lawyer that you will associate with in above case.</i>	
Lawyer's Minnesota License Number	#MN0326689

**MINNESOTA PRO HAC VICE APPLICATION**180 EAST 5TH STREET, SUITE 950
ST. PAUL, MN 55101**QUESTIONS / AFFIRMATIONS**

Minnesota Rule of Professional Conduct 5.5(b)

YES

I affirm that I have read and reviewed Minnesota Rule of Professional Conduct [5.5\(b\)](#) and confirm that I do not have a systematic and continuous presence in Minnesota.

Rules of Court

YES

I affirm that there are no disciplinary complaints currently filed against me in any jurisdiction for violation of the rules of court.

Suspended or Disbarred

YES

I affirm that I am not suspended or disbarred from practice for disciplinary reasons or reason of disability in lieu of discipline in any jurisdiction. I agree to promptly advise the court in which the matter is pending and the Board of Law Examiners if I become suspended or disbarred while the above matter is pending.

Times Previously Applied

None

*How many times have you previously applied for pro hac vice in Minnesota during the previous 12-Months? (Please see Rule [5.04\(a\)](#) for reporting requirements when submitting materials to the district court.)***FEE EXEMPTIONS**Application fees may be waived only if you qualify under [Rule 5.03\(b\)](#) of the Minnesota Rules of General Practice. No other requests for waiver will be reviewed.Applications do not need to be submitted for representation covered under [Rule 5.03\(a\)](#).

Limited Means

NO

I am representing a person with limited means and will not charge an attorney fee or seek or receive attorney fee reimbursement for the case in which I am seeking pro hac vice admission. [Rule 5.02\(b\)\(1\)](#)

Federal, State or Local Government Entity

NO

*I am a public attorney representing a federal, state, or local government. [Rule 5.02\(b\)\(2\)](#)***PAYMENT**

Pro Hac Vice Fee

\$450.00

PLEASE NOTE: The \$450 filing fee is allocated to the Legal Services Advisory Committee (LSAC) for civil legal services and grant program purposes. The bank processing fee is included in the \$450 payment. Applications must be submitted electronically. Application fees are non-refundable. Please review the Rules prior to submitting the application.Applications are typically processed within 24-72 business hours. An email confirming the application has been processed will be sent to the email address included in your application and your name will be added to the Minnesota Board of Law Examiners website under the Pro Hac Vice tab. You must still apply for *pro hac vice* through the Minnesota District Court handling the matter. See [Rule 5.04](#)

I declare under penalty of perjury that everything I have stated in this document is true and correct,

Date:

9/19/2021

Signature:

Terence R. Coates
Terence R. Coates

**THE SUPREME COURT OF MINNESOTA**

MINNESOTA BOARD OF LAW EXAMINERS
PRO HAC VICE APPLICATIONS
180 E. 5th Street, Suite 950
St. Paul, MN 55101

ProHacVice@mbcle.state.mn.us

651-297-1857

www.ble.mn.gov

September 20, 2021

Terence R. Coates

Markovits, Stock & DeMarco, LLC

3825 Edwards Road, Suite 650

Cincinnati, Ohio 45209

RE: Pro Hac Vice Application

Dear Attorney Coates:

This letter confirms that the office of the Minnesota Board of Law Examiners received the application for Pro Hac Vice admission from Terence R. Coates on 9/19/2021. The Board office has confirmed that the lawyer is in Good Standing in State of Ohio. Terence R. Coates has been added to the Minnesota Board of Law Examiners' website. If you have any questions, you may contact the Board at prohacvice@mbcle.state.mn.us.

This letter confirms that the fee has been paid or that the lawyer qualified for waiver of the fee pursuant to the Minnesota Rules of General Practice.

This application was submitted for Elizabeth Lutz: Case Number: 70-CV-21-11814 and the Minnesota Lawyer associated with the case is Bryan L. Bleichner; Lawyer License Number: #MN0326689.

Please refer to Minnesota Rule of General Practice 5.04 for additional information on what needs to be submitted to the District Court. Please note: the Court Rules require you to list on your Affidavit all applications for Pro Hac Vice in Minnesota for the preceding two years.

Very truly yours,
Minnesota Board of Law Examiners

State of Minnesota

County

Scott

District Court

Judicial District:

First

Court File Number:

70-CV-21-11814

Case Type:

Civil Other/Misc.

ELIZABETH LUTZ, individually and on
behalf of all others similarly situated,

Plaintiff/ Petitioner

vs./and

**ORDER REGARDING
PRO HAC VICE**ELECTROMED, INC.

Defendant/ Respondent

THE COURT FINDS:

1. A Motion for Admission of Pro Hac Vice was filed by: Bryan L. Bleichner,
an attorney admitted to practice in Minnesota.
2. The proposed admittee, Terence R. Coates, is an attorney
admitted to practice in the trial courts of Minnesota, but not admitted to
the bar of this court. The attorney will be counsel for the ☒ Plaintiff/Petitioner
☐ Defendant/Respondent.
3. The following documents have been submitted:
 - ☒ Copy of Application submitted under Rule 5.03 to the Minnesota Board of Law
Examiners;
 - ☒ Copy of the Notice from the Board of Law Examiners confirming good standing.
4. Other: _____

(Include findings to support denial)**IT IS ORDERED:**

1. The Court ☐ Grants ☐ Denies the motion for Pro Hac Vice in the above entitled matter.

BY THE COURT:

Dated: _____

Judge of District Court

Note: This order must be filed with the Court Administrator before you will receive notices
generated in this action.

State of Minnesota

County

Scott

District Court

Judicial District:

First

Court File Number:

70-CV-21-11814

Case Type:

Civil Other/Misc.

ELIZABETH LUTZ, individually and on
behalf of all others similarly situated,

Plaintiff/ Petitioner

vs./and

**ORDER REGARDING
PRO HAC VICE**

ELECTROMED, INC.

Defendant/ Respondent

THE COURT FINDS:

1. A Motion for Admission of Pro Hac Vice was filed by: Bryan L. Bleichner,
an attorney admitted to practice in Minnesota.
2. The proposed admittee, Terence R. Coates, is an attorney
admitted to practice in the trial courts of Ohio, but not admitted to
the bar of this court. The attorney will be counsel for the ☒ Plaintiff/Petitioner
☐ Defendant/Respondent.
3. The following documents have been submitted:
☒ Copy of Application submitted under Rule 5.03 to the Minnesota Board of Law
Examiners;
☒ Copy of the Notice from the Board of Law Examiners confirming good standing.
4. Other: _____

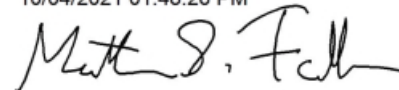
(Include findings to support denial)

IT IS ORDERED:

1. The Court ☒ **grants** ☐ **Denies** the motion for Pro Hac Vice in the above entitled matter.

BY THE COURT:

10/04/2021 01:48:26 PM



Dated: _____

Judge of District Court

Note: This order must be filed with the Court Administrator before you will receive notices
generated in this action.

STATE OF MINNESOTA

DISTRICT COURT

COUNTY OF SCOTT

FIRST JUDICIAL DISTRICT

CASE TYPE: Civil/Other Contracts

ELIZABETH LUTZ, on behalf of himself
and all others similarly situated,

Plaintiff,

v.

ELECTROMED, INC.,

Defendant.

Court File No. 70-CV-21-11814

Supplemental Civil Cover Sheet
(Non-Family Case Type)
Minn. R. Gen. P. 104

The following information was not known at the time the initial cover sheet was filed and is being supplied herein by Plaintiff's counsel as a Supplement to the Initial Cover Sheet filed on September 14, 2021:

ATTORNEY FOR DEFENDANT

Daniel R. Hall (#MN0392757)
Brooke D. Anthony (#MN0387559)
Anthony Ostlund Louwagie Dressen
Boylan P.A.
90 South 7th Street, Suite 3600
Minneapolis, MN 55402
Telephone: (612) 349-6969
dhall@anthonyostlund.com
banthony@anthonyostlund.com

Note: If either Plaintiff or Defendant gets an attorney, the attorney's name, address, telephone number and attorney ID number must be given in writing to the Court Administrator immediately.

By signing below, the attorney or party submitting this form certifies that the above information is true and correct.

Submitted by:

Dated: October 5, 2021

By: /s/ Bryan L. Bleichner
Bryan L. Bleichner (#MN0326689)
Christopher P. Renz (#MN0313415)
CHESTNUT CAMBRONNE PA
100 Washington Ave. S., Ste. 1700
Minneapolis, MN 55401-2138
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com
crenz@chestnutcambronne.com

Nathan D. Prosser (#MN0329745)
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
nprosser@hjlawfirm.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO,
LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Telephone: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

* *Pro Hac Vice* application filed

**Chestnut Cambronne PA**

100 Washington Avenue South
Suite 1700
Minneapolis, MN 55401
T: 612.339.7300
F: 612.336.2940

www.chestnutcambronne.com

Christopher P. Renz, Esq.
crenz@chestnutcambronne.com

October 5, 2021

VIA E-FILE

Scott County District Court
Attn: Court Administration
200 4th Ave W.
Shakopee, MN 55379

Re: Elizabeth Lutz et al. vs. Electromed, Inc.
Court File No.: 70-CV-21-11814
Our File No.: 20210763.000

Dear Sir/Madam,

My office represents Plaintiff Elizabeth Lutz in the above-referenced matter. This correspondence serves and a request for a jury trial. Should the court require anything in addition to this correspondence please let my office know. The \$100.00 jury fee will also be submitted along with this letter.

Thank you for your time and attention to this matter.

Sincerely,

CHESTNUT CAMBRONNE PA

A handwritten signature in blue ink, appearing to read 'C. Renz', written over a light blue horizontal line.

Christopher P. Renz
Attorney at Law

Scott County District Court

Page 2

cc: Bryan L. Bleichner, Esq. (by e-serve only)
Terence R. Coates, Esq. (by e-mail only)
Nathan D. Prosser, Esq. (by e-mail only)
Daniel R. Hall, Esq. (by e-mail only)

STATE OF MINNESOTA

DISTRICT COURT

COUNTY OF SCOTT

FIRST JUDICIAL DISTRICT

CASE TYPE: Civil/Other Contracts

ELIZABETH LUTZ, on behalf of himself
and all others similarly situated,

Plaintiff,

v.

ELECTROMED, INC.,

Defendant.

Court File No. 70-CV-21-11814

Supplemental Civil Cover Sheet
(Non-Family Case Type)
Minn. R. Gen. P. 104

The following information was not known at the time the initial cover sheet was filed and is being supplied herein by Plaintiff's counsel as a Supplement to the Initial Cover Sheet filed on September 14, 2021:

ATTORNEY FOR DEFENDANT

Daniel R. Hall (#MN0392757)
 Brooke D. Anthony (#MN0387559)
 Anthony Ostlund Louwagie Dressen
 Boylan P.A.
 90 South 7th Street, Suite 3600
 Minneapolis, MN 55402
 Telephone: (612) 349-6969
 dhall@anthonyostlund.com
 banthony@anthonyostlund.com

Note: If either Plaintiff or Defendant gets an attorney, the attorney's name, address, telephone number and attorney ID number must be given in writing to the Court Administrator immediately.

By signing below, the attorney or party submitting this form certifies that the above information is true and correct.

Submitted by:

Dated: October 5, 2021

By: /s/ Bryan L. Bleichner
Bryan L. Bleichner (#MN0326689)
Christopher P. Renz (#MN0313415)
CHESTNUT CAMBRONNE PA
100 Washington Ave. S., Ste. 1700
Minneapolis, MN 55401-2138
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com
crenz@chestnutcambronne.com

Nathan D. Prosser (#MN0329745)
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
nprosser@hjlawfirm.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO,
LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Telephone: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

* *Pro Hac Vice* application filed

STATE OF MINNESOTA

DISTRICT COURT

COUNTY OF SCOTT

FIRST JUDICIAL DISTRICT

CASE TYPE: CIVIL/OTHER CONTRACTS

ELIZABETH LUTZ, *individually and on
behalf of all others similarly situated,*

Plaintiff,

v.

ELECTROMED, INC.

Defendant.

Case No. 70-CV-21-11814

**FIRST AMENDED
CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Elizabeth Lutz, individually and on behalf of all others similarly situated, brings this action against Defendant Electromed, Inc. (“Defendant” or “Electromed”), a Minnesota corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack and data breach in June 2021 (“Data Breach”) on Defendant’s network that resulted in unauthorized access to customer and employee data. As a result of the Data Breach, Plaintiff and approximately 47,200 Class Members¹ suffered ascertainable losses in the form of the loss of the benefit of their bargain,

¹ See *Cases Currently Under Investigation*, Office for Civil Rights, U.S. Dept. of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Aug. 24, 2021).

out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

2. In addition, Plaintiff and Class Members' sensitive personal information—which was entrusted to Electromed, its officials and agents—was compromised and unlawfully accessed due to the Data Breach.

3. Information compromised in the Data Breach includes Defendant's customers' first and last names, mailing addresses, medical information (including regarding medical history, mental or physical condition, and/or treatment), and health insurance information (collectively, "Private Information"), referred to by Defendant in its notice to Plaintiff of the Data Breach as "protected health information."

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained.

5. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

6. Plaintiff and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based on their individual health needs, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

9. Plaintiff and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

11. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims on behalf of the Class (defined *infra*) for negligence and negligence *per se*. Plaintiff also brings claims on behalf of the Subclass (defined *infra*) for claims under the California Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq.*, and the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code §1798.100, *et seq.*

JURISDICTION AND VENUE

13. This Court has jurisdiction over this action pursuant to Minn. Const. art. VI, § 3 and Minn. Stat. § 484.01, subd. 1.

14. This Court has original jurisdiction of this action because Defendant (a) is incorporated in Minnesota with the majority of its business in the State of Minnesota, (b) maintains its principal place of business in Minnesota, (c) is registered to do business in Minnesota, (d) is doing business in Minnesota, (e) committed the unlawful acts in Minnesota and (f) caused the resulting injury in Minnesota. Defendant is subject to the personal and general jurisdiction of this Court.

15. Venue is proper in this Court pursuant to Minn. Stat. § 542.09 because Defendant's principal place of business is located in the City of New Prague, County of Scott, State of Minnesota.

16. Upon information and belief, Plaintiff's individual damages do not exceed \$75,000, exclusive of costs and interest.

PARTIES

17. Plaintiff Elizabeth Lutz is, and at all times mentioned herein was, an individual citizen of the State of California. Plaintiff received a data breach notice letter dated August 9, 2021 informing her that her "protected health information, such as [her] first and last name, full mailing address, medical, and health insurance information" were compromised in the Data Breach.

18. As a result of the Data Breach, Plaintiff has experienced a significant increase in the number of fraudulent and/or unsolicited communications received. She estimates that since the Data Breach, she has spent up to an hour each day dealing with unsolicited (and often fraudulent) emails, text messages, and phone calls. This includes, on average, more than 40 unsolicited and/or

fraudulent emails per day. Despite attempting to “unsubscribe” from these emails, they persist. She has also received several emails stating that loans have been approved in her name (despite not applying for loans). As a result of the volume of unsolicited and/or fraudulent emails, she is forced to discontinue use of her account.

19. Defendant Electromed is a large publicly traded corporation incorporated under the laws of the State of Minnesota with its principal place of business located in New Prague, Minnesota.

DEFENDANT’S BUSINESS

20. Electromed engages in the development, manufacture, marketing, and sale of medical equipment. It offers SmartVest[®], an airway clearance system, to patients with compromised pulmonary function. Defendant focuses on building market awareness, and acceptance of its products and services with physicians, clinicians, patients, and third-party payers.

21. On information and belief, in the ordinary course of business, Electromed requires customers to provide sensitive personal and private information² such as:

- Full Name;
- Residential address;
- Medical information; and
- Health insurance information.

22. As part of the process of obtaining products and services from Defendant, Plaintiff provided Defendant with an extensive medical history, lists of medications, primary care physician and diagnostic information, as well as diagnoses and test results from multiple physicians. The

² <https://smartvest.com/wp-content/uploads/2017/12/SmartVest-Required-Prescription-Documentation.pdf> (last visited Aug, 26, 2021).

medical information and Medicare insurance information Plaintiff provided likely contained her Social Security Number, in addition to other Private Information.

23. While Defendant has admitted that some “protected health information” was accessed, it is also believed that Defendant acquired and stored Plaintiff’s and Class Members’ Social Security numbers, the theft of which would leave Plaintiff and Class Members open to even further risks of identity theft.

24. On further information and belief, Electromed provides each of its customers with a HIPAA compliant notice titled “NOTICE OF PRIVACY PRACTICES OF ELECTROMED, INC., A HEALTHCARE PROVIDER” (the “Privacy Notice”) that explains how it handles customers’ sensitive and confidential information.³

25. The Privacy Notice is provided to every customer upon request and is posted on Defendant’s website.⁴

26. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to its customers, Electromed promises to, among other things: develop and maintain “appropriate administrative, technical, and physical safeguards necessary to maintain confidentiality” of protected health information (“PHI”); inform customers of its legal duties and comply with laws protecting customers’ health information; only use and release customers’ health information for approved reasons, and adhere to the terms outlined in the Privacy Notice.⁵

27. As a condition of purchasing goods and services from Defendant, Electromed requires that its customers entrust it with highly sensitive personal information.

³ <https://smartvest.com/wp-content/uploads/2017/12/Electromed-Notice-of-Privacy-Practices.pdf> (last visited Aug. 26, 2021).

⁴ *Id.*

⁵ *Id.*

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' Private Information from unauthorized disclosure.

29. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

30. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE CYBERATTACK AND DATA BREACH

31. On or about June 16, 2021, Electromed discovered suspicious activity on its IT systems.⁶

32. Following the discovery of suspicious activity, Electromed launched an investigation, which concluded that unauthorized third parties accessed files containing the sensitive personal and protected health information of its customers, employees, and certain third-party contractors.⁷

33. In addition, the investigation revealed that approximately 47,200 individuals were victims of the Data Breach.⁸

34. Defendant had obligations created by the Health Insurance Portability and Accountability Act ("HIPAA"), contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members that it would keep their Private

⁶ <https://www.hipaajournal.com/phi-of-47000-individuals-potentially-compromised-in-electromed-inc-data-breach/> (last visited Aug. 26, 2021).

⁷ *Id.*

⁸ *Id.*

Information confidential and protect it from unauthorized access and disclosure.

35. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

36. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

37. In light of recent high-profile data breaches at other companies in the healthcare industry, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

38. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."⁹

39. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.¹⁰

40. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

⁹ *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited June 23, 2021).

¹⁰ See Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, Security Magazine (Nov. 23, 2020), <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack> (last visited Aug. 24, 2021).

Defendant Fails to Comply with FTC Guidelines

50. The Federal Trade Commission (“FTC”) has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.¹¹ The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.¹²

52. The FTC further recommends that companies: not maintain personally identifiable information (“PII”) longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

¹¹ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 24, 2021).

¹² *Id.*

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

54. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”)

55. Defendant failed to properly implement basic data security practices.

56. Defendant’s failure to employ reasonable and appropriate measures to protect against and detect unauthorized access to customers’ PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

57. Defendant was at all times fully aware of its obligation to protect the PII and PHI of their customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

58. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

59. Several best practices have been identified that a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software;

encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

60. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

61. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

62. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security

63. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

64. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

65. Title II of HIPAA contains what are known as the Administrative Simplification

provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other things, that the Department of Health and Human Services (“HHS”) create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

66. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

A breach under the HIPAA Rules is defined as, “the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI.” *See* 45 C.F.R. § 164.40

67. Defendant’s Data Breach resulted from a combination of insufficiencies that demonstrate Electromed failed to comply with safeguards mandated by HIPAA regulations.

DEFENDANT’S BREACH

68. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant’s unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect customers’ Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;

- d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- e. Failing to train its employees in the proper handling of emails containing PII and PHI and maintain adequate email security practices;
- f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);
- i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);
- j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

- l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);
- m. Failing to train all members of its workforces effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);
- n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” (45 CFR § 164.304’s definition of “encryption”);
- o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and
- p. Failing to adhere to industry standards for cybersecurity.

69. Defendant negligently and unlawfully failed to safeguard Plaintiff and Class Members’ Private Information by allowing cyberthieves to access Electromed’s computer network and systems which contained unsecured and unencrypted PII.

70. Accordingly, as outlined below, Plaintiff and Class Members now face a present and substantially increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at a Present and Substantially Increased Risk of Fraud and Identity Theft

71. Cyberattacks and data breaches at healthcare providers like Defendant are

especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

72. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.¹³

73. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.¹⁴

74. The United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”¹⁵

75. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and take over victims’ identities in order to engage in illegal financial transactions under the victims’ names. Because a person’s identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person,

¹³ See Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), <https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks> (last visited Aug. 24, 2021).

¹⁴ See Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at <https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203> (last visited Aug. 25, 2021).

¹⁵ See U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007). Available at <https://www.gao.gov/new.items/d07737.pdf> (last visited Aug. 25, 2021).

the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

76. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.¹⁶

77. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

78. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

¹⁶ See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/#/Steps> (last visited Aug. 25, 2021).

79. Moreover, theft of Private Information is also gravely serious. PII and PHI is an extremely valuable property right.¹⁷

80. Its value is axiomatic, considering the value of “big data” in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

81. Theft of PHI, in particular, is gravely serious: “[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief’s health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.”¹⁸

82. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII and PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves.

83. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

84. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen

¹⁷ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

¹⁸ See Federal Trade Commission, *Medical Identity Theft*, <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft> (last visited Aug. 25, 2021).

data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

85. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

86. There is a strong probability that entire batches of information stolen from Defendant have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at a present and substantially increased risk of fraud and identity theft for many years into the future.

87. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

88. Sensitive Private Information can sell for as much as \$363 per record according to the Infosec Institute.¹⁹ PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

89. For example, the Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines.²⁰ Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for

¹⁹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Aug. 25, 2021).

²⁰ *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Aug. 25, 2021).

unemployment benefits, or apply for a job using a false identity.²¹ Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

90. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

91. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”²²

92. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”²³

93. Medical information is especially valuable to identity thieves.

94. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just \$1 in 2016 – the same as a Facebook account.²⁴ That

²¹ *Id.* at 4.

²² Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Aug. 25, 2021).

²³ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Aug. 25, 2021).

²⁴ See Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), <https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/> (last visited Aug. 25, 2021).

pales in comparison with the asking price for medical data, which was selling for \$50 and up.²⁵

95. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

96. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Electromed failed to properly prepare for that risk.

Plaintiff and Class Members' Damages

97. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

98. Defendant has merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to twelve (12) months, but this does nothing to compensate them for damages incurred and time spent dealing with the Data Breach.

99. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

100. Plaintiff's Private Information was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's computer system.

101. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach.

²⁵ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last visited Aug. 25, 2021).

102. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

103. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

104. Plaintiff and Class Members face the present and substantially increased risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

105. Plaintiff and Class Members face the present and substantially increased risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

106. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

107. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

108. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service or product that was intended to be accompanied by adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Electromed's

computer network and Plaintiff and Class Members' Private Information. Thus, Plaintiff and the Class Members did not get what they paid for and agreed to.

109. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and sensitive information for misuse.

110. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing "freezes" and "alerts" with reporting agencies;
- d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts; and,
- f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

111. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not

limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

112. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

CLASS ACTION ALLEGATIONS

113. Plaintiff brings this action on behalf of themselves and on behalf of all other persons similarly situated (“the Class”).

114. Plaintiff proposes the following Class and California Subclass definitions, subject to amendment as appropriate:

All persons Electromed identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the “Class”).

All residents of California who Electromed identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the “California Subclass”).

115. The Class and California Subclass are referred to collectively as the “Classes.” Members of the Classes are referred to collectively as “Class Members.”

116. Excluded from the Classes are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

117. Plaintiff reserves the right to amend or modify the Class definitions as this case progresses.

118. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately 47,200 individuals whose sensitive data, including private personal and medical information was compromised in the Data Breach. Upon information and belief, the California Subclass consists of more than 500 individuals whose sensitive data was compromised in the Data Breach.

119. Commonality. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff and Class Members' Private Information;
- b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, HIPAA;
- d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

- f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;
- h. Whether Defendant should have discovered the Data Breach sooner;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant breached a fiduciary duty to Plaintiff and Class Members;
- l. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and
- m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, treble damages, and/or injunctive relief.

120. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

121. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's Counsel are competent and experienced in litigating class actions.

122. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from

Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

123. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

124. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

FIRST COUNT

Negligence

(On Behalf of Plaintiff and the Classes)

125. Plaintiff re-alleges and incorporates by reference all other paragraphs in paragraphs 1 through 124 of the Complaint as if fully set forth herein.

126. Defendant required customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of rendering healthcare goods and services.

127. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members’ Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant’s duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

128. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

129. Defendant’s duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

130. Defendant’s duty to use reasonable security measures under HIPAA required Defendant to “reasonably protect” confidential data from “any intentional or unintentional use or disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes “protected health information” within the meaning of HIPAA.

131. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

132. Defendant’s duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

133. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members’ Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members’ Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Failing to have in place mitigation policies and procedures;
- e. Allowing unauthorized access to Class Members’ Private Information;
- f. Failing to detect in a timely manner that Class Members’ Private Information had been compromised; and
- g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

134. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

135. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

136. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

137. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Negligence *Per Se*
(On Behalf of Plaintiff and the Classes)

138. Plaintiff re-alleges and incorporates by reference all other paragraphs in paragraphs 1 through 137 of the Complaint as if fully set forth herein.

139. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

140. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's

conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

141. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

142. Plaintiff and members of the Class are within the class of persons that the FTC Act was intended to protect.

143. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

144. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect

the PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

145. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession.

THIRD COUNT

California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.* (On Behalf of Plaintiff and the California Subclass)

146. Plaintiff re-alleges and incorporates by reference all other paragraphs in paragraphs 1 through 145 of the Complaint as if fully set forth herein.

147. Defendant is a "contractor," as defined in Cal. Civ. Code §56.05(d) and "a provider of health care," as defined in Cal. Civ. Code §56.05(m), and is therefore subject to the requirements of the CMIA, Cal. Civ. Code §56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

148. Electromed is a person licensed under California under California's Business and Professions Code, Division 2. *See* Cal. Bus. Prof. Code § 4000, *et seq.* Electromed therefore qualifies as a "provider of health care" under the CMIA.

149. Plaintiff and the California Subclass are "patients" as defined in CMIA, Cal. Civ. Code §56.05(k) ("Patient" means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains."). Furthermore, Plaintiff and California Subclass members, as patients and customers of Defendant,

had their individually identifiable “medical information,” within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendant’s computer network, and were patients on or before June 16, 2021.

150. Electromed disclosed “medical information,” as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Electromed’s employees, which allowed the hackers to see and obtain Plaintiff’s and the California Subclass members’ medical information.

151. Electromed negligently created, maintained, preserved, stored, and then exposed Plaintiff’s and California Subclass members’ individually identifiable “medical information,” within the meaning of Cal. Civ. Code § 56.05(j), including Plaintiff’s and California Class members’ names, addresses, medical information, and health insurance information, that alone or in combination with other publicly available information, reveals their identities.

152. Electromed’s negligence resulted in the release of individually identifiable medical information pertaining to Plaintiff and the California Subclass to unauthorized persons and the breach of the confidentiality of that information. Electromed’s negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff’s and California Subclass members’ medical information in a manner that preserved the confidentiality of the information contained therein, in violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

153. Plaintiff’s and California Subclass members’ medical information was accessed and actually viewed by hackers in the Data Breach.

154. Plaintiff's and California Subclass members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

155. Electromed's computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A).

156. As a direct and proximate result of Electromed's above-noted wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiff and the California Subclass have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) present, imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of the PII and PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII and PHI, for which there is well-established national and international markets, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

157. Plaintiff and the California Subclass were injured and have suffered damages, as described above, from Electromed's illegal and unauthorized disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, which allows for actual damages, nominal statutory damages of \$1,000, punitive damages of \$3,000, injunctive relief, and attorneys' fees, expenses and costs.

FOURTH COUNT

**Violation of California's Consumer Protection Act, Cal. Civ. Code § 1798.150
(On behalf of Plaintiff and the California Class)**

158. Plaintiff re-alleges and incorporates by reference all other paragraphs in paragraphs 1 through 157 of the Complaint as if fully set forth herein.

159. Electromed had duties to implement and maintain reasonable security procedures and practices with regard to the PII and PHI of Plaintiff and the California Subclass.

160. Plaintiff Lutz and the California Subclass provided to Electromed their nonencrypted and nonredacted personal information as defined in Cal. Civ. Code § 1798.81.5 in the form of their PII.

161. Electromed violated the California Consumer Privacy Act ("CCPA") by failing to prevent the PII and PHI of Plaintiff and the California Subclass from unauthorized access and exfiltration, theft, or disclosure as a result of Electromed's violations of its duties to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII and PHI of Plaintiff and the California Subclass.

162. As a direct and proximate result of Electromed's acts, including, but not limited to, its failure to encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, the unencrypted and unredacted PII and PHI of Plaintiff and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Electromed's violation of its duties.

163. As a direct and proximate result of Electromed's acts, including, but not limited to, their failure to encrypt their systems and otherwise implement and maintain adequate and reasonable security procedures and practices, Plaintiff and the California Class Subclass were injured and lost money or property, including but not limited to the loss of the California Subclass's

legally protected interest in the confidentiality and privacy of their PII and PHI, nominal damages, and additional losses as described above.

164. Electromed knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII and PHI of Plaintiff and the California Subclass and that the risk of a data breach or theft was highly likely. Electromed failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII and PHI of Plaintiff and the California Subclass.

165. Electromed is a corporation organized for the profit or financial benefit of its owners, with annual gross revenues exceeding \$25 million, and collects PII and PHI as defined in Cal. Civ. Code § 1798.140.

166. Plaintiff and California Subclass members seek relief under § 1798.150(a), including, but not limited to, injunctive or declaratory relief, and any other relief the court deems proper, to ensure Electromed hereinafter adequately safeguards the PII and PHI of Plaintiff Lutz and the California Subclass by implementing reasonable security procedures and practices. Such relief is particularly important because Electromed continues to hold the PII and PHI of Plaintiff and the California Subclass. These individuals have an interest in ensuring that their PII is reasonably protected.

167. On September 2, 2021, Plaintiff provided written notice to Electromed identifying the specific provisions of this title he alleges they have violated. As of the date of filing this complaint, Electromed has not responded to Plaintiff's written notice and has failed to "actually cure" its violations of Cal. Civ. Code § 1798.150(a). Therefore, Plaintiff seeks statutory damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty

(\$750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

- a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representatives and their counsel as Class Counsel;
- b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information;
- c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII and PHI compromised during the Data Breach;
- d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- e) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;
- f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- h) Pre- and post-judgment interest on any amounts awarded; and
- i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: October 4, 2021

Respectfully Submitted,

/s/ Bryan L. Bleichner

Bryan L. Bleichner (MN 0326689)

Christopher P. Renz (MN 0313415)

CHESTNUT CAMBRONNE PA

100 Washington Avenue South, Suite 1700

Minneapolis, MN 55401

Phone: (612) 339-7300

bbleichner@chestnutcambronne.com

crenz@chestnutcambronne.com

Nathan D. Prosser (MN 0329745)

HELLMUTH & JOHNSON, PLLC

8050 West 78th Street

Edina, MN 55439

Telephone: (952) 941-4005

nprosser@hjlawfirm.com

Terence R. Coates (*pro hac vice* pending)

Dylan J. Gould (*pro hac vice* forthcoming)

MARKOVITS, STOCK & DEMARCO, LLC

3825 Edwards Road, Suite 650

Cincinnati, OH 45209

Phone: (513) 651-3700

tcoates@msdlegal.com

dgould@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

ACKNOWLEDGEMENT

The undersigned hereby acknowledges that costs, disbursements, and reasonable attorneys' and witness fees may be awarded pursuant to Minn. Stat. § 549.211, to the parties against whom the allegations in this pleading are asserted.

Dated: October 4, 2021

/s/ *Bryan L. Bleichner*
Bryan L. Bleichner (#0326689)

STATE OF MINNESOTA

AFFIDAVIT OF SERVICE

COUNTY OF HENNEPIN

Re: ELIZABETH LUTZ, ET AL.

V,

ELECTROMED, INC.

Court File No.:

Our File No:

John Pothen, being first duly sworn upon oath, deposes and states, that on the 7th day of **September, 2021**, he served:

- 1. SUMMONS; AND**
- 2. CLASS ACTION COMPLAINT,**

upon **ELECTROMED, INC.**, therein named at, **502 – 6th Avenue NW, New Prague**, County of **Scott**, State of **Minnesota**, by handing true and correct copies thereof with **Kathleen S. Skarvan, CEO**.

Subscribed and Sworn to before me
this 8th day of **September, 2021**.


Notary Public




John Pothen
Process Server

STATE OF MINNESOTA

DISTRICT COURT

COUNTY OF SCOTT

FIRST JUDICIAL DISTRICT

CASE TYPE: CIVIL/OTHER CONTRACTS

Case No. 70-CV-21-11814

*ELIZABETH LUTZ, individually and on
behalf of all others similarly situated,*

Plaintiff,

v.

ELECTROMED, INC.

Defendant.

CERTIFICATE OF REPRESENTATION

Pursuant to Rule 104 of the General Rules of Practice for District Courts, this form must be completed and filed with the Court Administrator's Office at the time the case is filed. The court administrator shall, upon receipt of the completed certificate, notify all parties or their lawyers of the date of filing the action and the file number assigned.

LIST ALL LAWYERS/PRO SE PARTIES INVOLVED IN THIS CASE**LAWYER FOR PLAINTIFF**/s/ Bryan L. Bleichner

Bryan L. Bleichner (MN 0326689)

Christopher P. Renz (MN 0313415)

CHESTNUT CAMBRONNE PA

100 Washington Avenue South, Suite 1700

Minneapolis, MN 55401

Phone: (612) 339-7300

*bbleichner@chestnutcambronne.com**crenz@chestnutcambronne.com*

Nathan D. Prosser (MN 0329745)

HELLMUTH & JOHNSON, PLLC

8050 West 78th Street

Edina, MN 55439

Telephone: (952) 941-4005

nprosser@hjlawfirm.com

Terence R. Coates (pro hac vice forthcoming)

Dylan J. Gould (pro hac vice forthcoming)

**MARKOVITS, STOCK & DEMARCO,
LLC**

3825 Edwards Road, Suite 650

Cincinnati, OH 45209

Phone: (513) 651-3700

*tcoates@msdlegal.com**dgould@msdlegal.com*

Dated: September 13, 2021

s/ Bryan L. Bleichner

Bryan L. Bleichner

Attorney for Plaintiff

STATE OF MINNESOTA

DISTRICT COURT

COUNTY OF SCOTT

FIRST JUDICIAL DISTRICT

CASE TYPE: Civil/Other Contracts

ELIZABETH LUTZ, on behalf of himself
and all others similarly situated,

Plaintiff,

v.

ELECTROMED, INC.,

Defendant.

Court File No. _____

Civil Cover Sheet
(Non-Family Case Type)
Minn. R. Gen. P. 104Date Case Filed: September 8, 2021

This civil cover sheet must be filed by the initial filing lawyer or party, if unrepresented by legal counsel, unless the court orders all parties or their legal counsel to complete this form. Once the initial civil cover sheet is filed, opposing lawyers or unrepresented parties who have not already been ordered to complete this form may submit their own cover sheet within 7 days after being served with the initial cover sheet. See Rule 104 of the General Rules of Practice for the District Courts.

If information is not known to the filing party at the time of filing, it shall be provided to the Court Administrator in writing by the filing party within seven (7) days of learning the information. Any party impleading additional parties shall provide the same information to the Court Administrator. The Court Administrator shall, upon receipt of the completed certificate, notify all parties or their lawyers, if represented by counsel, of the date of filing the action and the file number assigned.

**ATTORNEYS FOR PLAINTIFF
AND THE PROPOSED CLASS**

ATTORNEY FOR DEFENDANT

Bryan L. Bleichner (#MN0326689)
Christopher P. Renz (#MN0313415)
CHESTNUT CAMBRONNE PA
100 Washington Ave. S., Ste. 1700
Minneapolis, MN 55401-2138
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com
crenz@chestnutcambronne.com

Nathan D. Prosser (#MN0329745)
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
nprosser@hjlawfirm.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO,
LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Telephone: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

* *Pro hac vice* application to be promptly
filed

Note: If either Plaintiff or Defendant gets an attorney, the attorney's name, address, telephone number and attorney ID number must be given in writing to the Court Administrator immediately.

1. Provide a concise statement of the case including facts and legal basis:

This is a class action lawsuit initiated by the Plaintiff who was one of many people whose sensitive personal information, which was entrusted to Defendant, was compromised and unlawfully accessed during a data breach in June 2021. The information compromised in the data breach included full names, mailing addresses, medical and health insurance information. Plaintiff alleges that Defendant was negligent in the manner in which it maintained the private information of Plaintiff and others in the class. Plaintiff seeks to remedy the harms on behalf of herself and those similarly situated in the class. Plaintiff brings causes of action for negligence, negligence per se, and violation of the California Consumer Privacy Act and the California Confidentiality of Medical Information Act.

2. Date Complaint was served: September 8, 2021

3. For Expedited Litigation Track (ELT) Pilot Courts only: N/A

4. For Complex Cases (See Minn. Gen. R. Prac. 146):

a. Is this a "complex case" as defined by Rule 146? Yes

b. State briefly the reasons for complex case treatment for this case:

This is a complex consumer protection class action.

c. Have the parties filed a "CCP Election" for this case as provided in Rule 146(d)?

☐ No ☒ Yes

5. Estimated discovery completion within **12 months** from the date of this form.

6. Disclosure / discovery of electronically stored information discussed with other party?

☒ **No** ☐ Yes

If Yes, list agreements, plans, and disputes: N/A

7. Proposed trial start date: **February 1, 2023.**

8. Estimated trial time: **10 days** (estimates less than a day must be stated in hours).

9. Jury trial is:

☐ waived by consent of _____ pursuant to Minn. R. Civ. P. 38.02.

☒ requested by **Plaintiff** (NOTE: Applicable fee must be enclosed)

10. Physical/mental/blood examination pursuant to Minn. R. Civ. P. 35 is requested:
☐ Yes ☒ **No**
11. Identify any party or witness who will require interpreter services, and describe the services needed (specifying language, and if known, particular dialect):
Plaintiff is not aware of any interpreter services needed at this time.
12. Issues in dispute:
Whether Defendant acted negligently in the manner in which it stored sensitive personal and health information; whether a class should be certified; and the appropriate relief to Plaintiff and the class.
13. Case Type / Category: **Civil/Other Contracts**
14. Recommended Alternative Dispute Resolution (ADR) mechanism: **Mediation**
(See list of ADR processes set forth in Minn. Gen. R. Prac. 114.02(a))
Recommended ADR provider (known as a "neutral"): **N/A**
Recommended ADR completion date: **August 1, 2023**
If applicable, reasons why ADR not appropriate for this case: _____

By signing below, the attorney or party submitting this form certifies that the above information is true and correct.

Submitted by:

Dated: September 14, 2021

By: /s/ Bryan L. Bleichner
Bryan L. Bleichner (#MN0326689)
Christopher P. Renz (#MN0313415)
CHESTNUT CAMBRONNE PA
100 Washington Ave. S., Ste. 1700
Minneapolis, MN 55401-2138
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com
crenz@chestnutcambronne.com

Nathan D. Prosser (#MN0329745)
HELLMUTH & JOHNSON, PLLC

8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
nprosser@hjlawfirm.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO,
LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Telephone: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

* *Pro Hac Vice* application to be promptly filed

STATE OF MINNESOTA

DISTRICT COURT

COUNTY OF SCOTT

FIRST JUDICIAL DISTRICT
Case Type: Civil/Other ContractsELIZABETH LUTZ, individually and
on behalf of all others similarly situated,

Plaintiff,

vs.

ELECTROMED, INC.,

Defendant.

Court File No. 70-CV-21-11814

COMPLEX CASE PROGRAM
ELECTION FORM
(MINN. R. GEN. P. 146)

Date Case Filed: September 8, 2021

Each party who has signed this document has read and understands the Complex Case Program (CCP) Rule 146 and agrees that this case may be governed by the CCP.

Plaintiff Elizabeth Lutz through counsel:

Bryan L. Bleichner (#MN0326689)
Christopher P. Renz (#MN0313415)
CHESTNUT CAMBRONNE PA
100 Washington Ave. S., Ste. 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com
crenz@chestnutcambronne.com

Nathan D. Prosser (#MN0329745)
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
nprosser@hjlawfirm.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO,
LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Telephone: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

**Pro Hac Vice Applications to be filed*

Dated: September 14, 2021

Respectfully submitted,

By: /s/ Bryan L. Bleichner
Bryan L. Bleichner (#MN0326689)
Christopher P. Renz (#MN0313415)
CHESTNUT CAMBRONNE PA
100 Washington Ave. S., Ste. 1700
Minneapolis, MN 55401-2138
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com
crenz@chestnutcambronne.com

Nathan D. Prosser (#MN0329745)
HELLMUTH & JOHNSON, PLLC
8050 West 78th Street
Edina, MN 55439
Telephone: (952) 941-4005
nprosser@hjlawfirm.com

Terence R. Coates*
Dylan J. Gould*
MARKOVITS, STOCK & DEMARCO,
LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Telephone: (513) 651-3700
tcoates@msdlegal.com
dgould@msdlegal.com

Attorneys for Plaintiff and the Proposed Class

* *Pro Hac Vice* application to be promptly filed

State of Minnesota
Scott County

District Court
First Judicial District

Court File Number: **70-CV-21-11814**

Case Type: Civil Other/Misc.

Notice of Case Filing

FILE COPY

Elizabeth Lutz, individually and on behalf of all others similarly situated vs Electromed, Inc.

Date Case Filed: **09/08/2021**

Court file number **70-CV-21-11814** has been assigned to this matter. All future correspondence must include this file number, the attorney identification number, and must otherwise conform to format requirements or they WILL BE RETURNED. Correspondence and communication on this matter should be directed to the following court address:

**Scott County Court Administration
200 4th Avenue West JC 115
Shakopee MN 55379
952-496-8200**

If ADR applies, a list of neutrals is available at www.mncourts.gov (go to Alternative Dispute Resolution) or at any court facility.

Dated: September 15, 2021

Vicky L. Carlson
Court Administrator
Scott County District Court

cc: Electromed, Inc.
BRYAN L BLEICHNER